

**DISTRICT COURT OF THE VIRGIN ISLANDS
DIVISION OF ST. THOMAS & ST. JOHN**

UNITED STATES OF AMERICA,)	
)	
vs.)	Criminal №.: 3:13-CR-00022-CVG-RM-4
)	
ROBERTO TAPIA,)	Magistrate №.: 3:13-MJ-00026-CVG-RM
ANGELO HILL,)	
STEPHEN TORRES,)	
EDDIE LOPEZ LOPEZ,)	
RAYMOND BROWN, and)	
EDWIN MONSANTO,)	
)	
Defendants.)	
)	

MOTION TO SUPPRESS CELL SITE INFORMATION

COMES NOW Defendant, EDDIE LOPEZ LOPEZ, by and through his undersigned counsel, pursuant to Federal Rules of Criminal Procedure 12, the Court's inherent powers, hereby files this Motion to Suppress pursuant to the Fourth Amendment, made applicable by the Revised Organic Act and the United States Constitution, and hereby states as follows:

I. FACTS

On April 13, 2013, AUSA Lake on behalf of the Government filed an Application for an order requesting both (1) a Pen Register and a Trap & Trace pursuant to 18 U.S.C. §§ 3122, 3133 and (2) information reflecting the location of cellular towers related to the target telephones (Cell Site Location Information, (CSLI)) pursuant to 18 U.S.C. § 2703(d). Case no. Misc. 13-49. The Application was accompanied by an Affidavit of Detective Querrard, a deputized Federal Task Force Office of the DEA. The Affidavit stated, in relevant part: "[i]t is necessary to identify the cell tower location of [telephone numbers] in order to interdict and seize the transportation of narcotics before reaching its intended destination in Puerto Rico." *Aff.* at p. 5.

USA V. LOPEZ LOPEZ, ET AL.
3:13-CR-00022-CVG-RM-4
MOTION TO SUPPRESS — CELL SITE INFORMATION

The Application requested, *inter alia*, that: “the Order authorize agents of the Investigative Agency to acquire, during the same 60-day period, cell-site information for communications to and from the Target Telephone as well as the physical location of the cellular tower(s) indentified thereby.” App. at p. 4. The Court granted the Application on April 13, 2013. As a result of the Order, the Government was able to locate and interdict the Defendant in the waters between Puerto Rico and St. Thomas.

II. APPLICABLE LAW

A. Technologic Background

Recent years have seen the emergence of many new devices that permit the monitoring of a person’s movements. In some locales, closed-circuit television video monitoring is becoming ubiquitous. On toll roads, automatic toll collection systems create a precise record of the movements of motorists who choose to make use of that convenience. Many motorists purchase cars that are equipped with devices that permit a central station to ascertain the car’s location at any time so that roadside assistance may be provided if needed and the car may be found if it is stolen. Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users—and as of June 2011, it has been reported, there were more than 322 million wireless devices in use in the United States.

United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, concurring) (internal citation omitted).

“Cellular telephone networks divide geographic areas into many coverage areas containing towers through which the cell phones transmit and receive calls. Cell phones, whenever on, now automatically communicate with cell towers, constantly relaying their location information to the towers that serve their network and scanning for the one that provides the strongest signal/best reception. This process, called “registration”, occurs approximately

every seven seconds.”[footnote in opinion]¹ *In re U.S. for an Order Directing a Provider of Elec. Comm’n Serv. to Disclose Records to the Gov’t*, 534 F. Supp. 2d 585, 589-90 (W.D. Pa. 2008) (hereinafter *Lenihan Op.*) *aff’d*, 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008) *vacated sub nom. In re Application of U.S. for an Order Directing a Provider of Elec. Comm’n Serv. to Disclose Records to Gov’t*, 620 F.3d 304 (3d Cir. 2010) (hereinafter *Slovitier Op.*).

As we change locations, our cell phones automatically switch cell towers. Cellular telephone companies “track the identity of the cell towers serving a phone”. When a call is received, a mobile telephone switching office (“MTSO”) gets the call and locates the user based on the nearest tower; the call is then sent to the phone via that tower. This process works in reverse when the user places a call. In urban areas, where towers have become increasingly concentrated, tracking the location of just the nearest tower itself can place the phone within approximately 200 feet. This location range can be narrowed by “tracking which 120 degree ‘face’ of the tower is receiving a cell phone’s signal.” The individual’s location is, however, most precisely determinable by triangulating the “TDOA” or “AOA” information of the three nearest cellular towers. Alternatively, the phone can be tracked extremely accurately within as little as 50 feet-via the built-in global positioning system (“GPS”) capabilities of over 90% of cell phones currently in use. See also *Who Knows Where You’ve Been?*, 18 Harv. J.L. & Tech. at 308 (noting that, as of 2004, synchronized signal triangulation produced a 3-D location accurate to 65 feet). CSPs store cell tower registration histories and other information.

Lenihan Op. at 590 (some internal citations omitted).

B. Statutory Framework

1. The Pen Register Statute

The Pen Register Statute (PRS) was enacted as Title III of the Electronic Communication

¹ These location signals are generally set on one band (often referred to as a “control channel”); the other frequency bands that the phone uses are for sending and receiving voice and data. See Kevin McLaughlin, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 Hastings Comm. & Ent. L.J. 421, 427 (Spring 2007); See also *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 750 (S.D. Tex. 2005) (hereinafter *Smith Op.*) (explaining that “control channels” are frequencies shared by the phone and base station to communicate information for setting up calls and channel changing, and that cell phone “registrations” occur “on a dedicated control channel that is clearly separate from that used for call content”).

USA V. LOPEZ LOPEZ, ET AL.
3:13-CR-00022-CVG-RM-4
MOTION TO SUPPRESS — CELL SITE INFORMATION

Privacy Act of 1986 (ECPA), codified at 18 U.S.C. §§ 3121-3127. The PRS applies to both Pen Registers and Trap & Trace devices (PRT&T). See 18 U.S.C. § 3121(a) (prohibiting the installation of PRT&T devices without a court order.

[A] “Pen Register” is a device which records or decodes electronic or other impulses which identify the telephone numbers dialed or otherwise transmitted on the telephone line to which such device is attached (i.e., the numbers of outgoing calls). A trap and trace device captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted (i.e., the numbers of incoming calls).

Lenihan Op., 534 F. Supp. 2d at 593.

The Government in accordance with the PSR must obtain a court order before using a PRT&T device. See 18 U.S.C. § 3121(a) (“[e]xcept as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order”). The issuing court must determine: “that the information likely to be obtained by [installing and using the device] is relevant to an ongoing criminal investigation.” 18 U.S.C. § 3121(a)(1). The temporal limit is 60 days, but can be extended upon application by the Government. 18 U.S.C. § 3132(c).

2. Store Communications Act

The Store Communications Act (SCA), codified at 18 U.S.C. §§ 2701-2711, was enacted as Title II of the ECPA regulates the disclosure of wire and electronic communications information. 18 U.S.C. § 2701(a). The SCA splits information requested by the Government into either: (A) contents of communications, 18 U.S.C. § 2703(a) and (b), or (B) “record[s] or other information pertaining to a subscriber to or customer of a [electronic communication service] (not including the contents of communications).” 18 U.S.C. § 2703(c).

USA V. LOPEZ LOPEZ, ET AL.
3:13-CR-00022-CVG-RM-4
MOTION TO SUPPRESS — CELL SITE INFORMATION

18 U.S.C. § 2703(c) provides the statutory requirements for compelled disclosure of “record[s] or other information pertaining to a subscriber to or customer of [an electronic communication or remote computing] service.” Subsection “c” gives the Government three ways to compel disclosure from a CSP: (A) a warrant under Fed. R. Crim. P. 41 (see 18 U.S.C. § 2703(c)(1)(A)); (B) consent of the customer to the disclosure (see 18 U.S.C. § 2703(c)(1)(C)); and (C) it can compel the disclosure if it receives an court order under § 2703(d) (see 18 U.S.C. § 2703(c)(1)(B)).

18 U.S.C. § 2703(d) states:

(d) Requirements for court order.—

A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

18 U.S.C. § 2703(d). The standard under § 2703(d) is substantially less than for a Rule 41 warrant.

The SCA is applicable only to “wire communications” or “electronic communications,” *see* 18 U.S.C. §§ 2701(a) and 2703, but CSLI does not meet the definition of a “wire communication,” *see* 18 U.S.C. § 2501(1) (defining “wire communication” as “any aural transfer made in whole or in part ... by the aid of wire, cable, or other like connection between the point of origin and the point of reception” (emphasis added)).

Further, the SCA excludes “any communication from a tracking device,” *see* 18 U.S.C. §2510(12)(C), from the definition of “electronic communication,” *see* 18 U.S.C. § 2510(12) (“electronic communication” is defined to include “any transfer of ... sounds[] [or] data ... transmitted in whole or in part by a ... radio, electromagnetic, photoelectronic or photooptical system”). A “tracking device” is “an electronic or mechanical device which permits the tracking of the movement of a person or object.” 18 U.S.C. § 3117(b).

3. The Communications Assistance for Law Enforcement Act

The Communications Assistance for Law Enforcement Act (CALEA) was enacted in 1994, codified at 47 U.S.C. §§ 1001-1010, and mandates that “telecommunications carrier[s] [to] ensure that [their] equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of,” *see* 47 U.S.C. § 1002(a)(2), *inter alia*:

(a) Capability requirements

Except as provided in subsections (b), (c), and (d) of this section and sections 1007(a) and 1008(b) and (d) of this title, a telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of—

(1) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government;

(2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier—

(A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and

(B) in a manner that allows it to be associated with the communication to which it pertains, except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of Title 18), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number);

47 U.S.C.A. § 1002(a)(1)-(2) (emphasis added).

“Call-identifying information” is defined by CALEA as “dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any ... telecommunications carrier.” 47 U.S.C. § 1001(2). The SCA and the CALEA consistently define “wire communication(s)” and “electronic communication(s)”, *see* 47 U.S.C. § 1001(1) (“[t]he terms defined in [18 U.S.C. § 2510] have, respectively, the meanings stated in that section.”)², *see* 18 U.S.C. § 2711(1) (“the terms defined in [18 U.S.C. § 2510] have, respectively, the definitions given such terms in that section.”). As with the SCA, under the CALEA communications from devices that can be used to track an individual’s location are not “electronic communications” under the CALEA. *See* 18 U.S.C. § 2510(12)(C) and 18 U.S.C. § 3117(b). As stated *supra* 18 U.S.C. § 3117(b) defines a “tracking device” as “an electronic or mechanical device which permits the tracking of the movement of a person or object.”

C. 4th Amendment Jurisprudence

The Fourth Amendment protects citizens from “unreasonable searches and seizures” of “their persons, houses, papers and effects.” U.S. Const, amend. IV. “What is reasonable depends upon all of the circumstances surrounding the search or seizure and the nature of the search or

² “Wire communication” and “electronic communication” are each defined in 18 U.S.C. § 2510(1) and (12), respectively.

USA v. LOPEZ LOPEZ, ET AL.
3:13-CR-00022-CVG-RM-4
MOTION TO SUPPRESS — CELL SITE INFORMATION

seizure itself.” *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985). There is a presumptive requirement that searches or seizures be carried out pursuant to a warrant. *See Katz v. United States*, 389 U.S. 347, 357 (1967) (“searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment -- subject only to a few specifically established and well -- delineated exceptions.”) (internal citations omitted).

“On a motion to suppress, the government bears the burden of showing that each individual act constituting a search or seizure under the Fourth Amendment was reasonable.” *United States v. Ritter*, 416 F.3d 256, 261 (3d Cir. 2005).

In order for there to be a Government seizure the movant must establish that he had an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as “reasonable.” *Katz*, 389 U.S. at 361 (Harlan, J., concurring). In *Katz* the Supreme Court concluded that Government’s placing of a wiretap on a public phone booth to record the contents of the criminal defendant’s phone call constituted a search, and finding that the government’s failure to obtain judicial authorization prior to engaging in that search violated the Fourth Amendment.

III. DISCUSSION AND ANALYSIS

Here, as detailed in the Application and Affidavit in support, the basis for the Order was to obtain on a prospective basis Cell-Site Location Information in order to actively track the location of the person or persons possessing the targeted cell phones. Indeed, as the Affidavit plainly acknowledges, the intent and need for the Order was to interdict on the open seas narcotics bound for Puerto Rico.

A. Order and Evidence was Obtain in Contravention of Statutory Authority**1. The Pen Register Statute Cannot Support *Prospective* Cell-Site Location Information.**

18 U.S.C. § 3127 provides for the statutory definitions of both Pen Registers and Trap & Trace devices. 18 U.S.C. § 3127(3) and (4). Each is defined as a device that captures, either for outgoing or incoming calls, “dialing, routing, addressing, or signaling information.” At first glance, CSLI appears to be “routing . . . or signaling information.” However, 47 U.S.C. § 1002 specifically excludes cellular tower location information from the reach of the pen register statutes. Accordingly, the PSR standing alone (or in combination, *see infra*) cannot authorize prospective CSLI.

2. Store Communications Act Cannot Support *Prospective* Cell-Site Location Information.

CSLI is unquestionably not contents of a “wire communication” or “electronic communication,” hence 18 U.S.C. § 2703(a) and (b) cannot apply. So the only possible basis for the disclosure to the Government of prospective CSLI is under 18 U.S.C. § 2703(c). But because CSLI is/are not a form of “wire communication,” as defined by statute³ the SCA can govern the disclosure of CSLI only if cellular communications can be classified as a form of “electronic communication.” But CSLI does not meet the definition of “electronic communication”⁴ because the SCA excludes “any communication from a tracking device” from the definition of “electronic communication.” *See* 18 U.S.C. § 2510(12)(C). A cellular phone meets the statutory definition of a “tracking device” because it is “an electronic or mechanical device which permits the tracking of the movement of a person or object.” 18 U.S.C. § 3117(b).

³ *See* 18 U.S.C. § 2501(1) (defining “wire communication” as “any aural transfer made in whole or in part ... by the aid of wire, cable, or other like connection between the point of origin and the point of reception” (emphasis added)).

⁴ *See* 18 U.S.C. § 2510(12) (“electronic communication” is defined to include “any transfer of ... sounds[] [or] data ... transmitted in whole or in part by a ... radio, electromagnetic, photoelectronic or photooptical system”).

Accordingly, when one reads the statutory provisions together one comes to one inescapable conclusion – the Government cannot obtain prospective CSLI pursuant to the SCA without a warrant. Accord 18 U.S.C. § 2703(c)(1)(A) (prohibiting the disclosure unless there is a Rule 41 warrant). Thus, the failure of the Government to obtain a Rule 41 warrant, in contrast to an order under § 2703(d), requires that the CSLI, and all evidence derived therefrom, be suppressed. *See* discussion *infra*.

3. The Communications Assistance for Law Enforcement Act Cannot Support *Prospective* Cell-Site Location Information.

The CALEA explicitly prohibits the Government from obtaining information under the PRS information that can be used to disclose the location of the subscriber. 47 U.S.C. § 1002(a)(2). And the CALEA defines the term “call-identifying information” as “dialing or signaling information that *identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any ... telecommunications carrier.*” 47 U.S.C. § 1001(2) (emphasis added).

Given that the CALEA, and the SCA, have the same statutory definitions of a “tracking device” and given the CALEA explicit prohibition on the Government obtaining information that can be used to locate the subscriber, i.e., CSLI, the CALEA cannot provide the Government with any basis to obtain CSLI. Indeed, Congress could not have been more explicit in its statutory limitations it placed on the Government for location information. Accordingly, the Government’s acquisition of CSLI was in contravention of the law and must be suppressed.

B. Cases Support the Position that *Prospective* Cell-Site Location Information Requires a Rule 41 Warrant.

Various courts around the country have rejected the Government’s use of prospective CSLI in order to track suspects, a survey of some of those follows.

In *In re Authorizing the Use of a Pen Register*, 384 F. Supp. 2d 562, 564 on reconsideration sub nom. *In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005) (hereinafter *Orenstein Op.*), that court stated: “[i]n other words, the requested information is useful in the same way that physical surveillance of the telephone user is useful: it reveals that person’s location at a given time. The fact that the request[] ... further suggests that the authorization, if granted, would effectively allow the installation of a tracking device without the showing of probable cause normally required for a warrant. The foregoing leads me to believe that I cannot grant the government the relief it seeks on the basis of the precise authority it cites, namely, 18 U.S.C. § 2703.”

In *Smith Op.*, supra at 757 that court stated: “[h]aving concluded that prospective cell site data is properly categorized as tracking device information under § 3117, the question arises whether such data may not also be obtainable under other provisions of the ECPA. In other words, do the four broad categories of the ECPA overlap, such that location information obtainable from a § 3117 tracking device is simultaneously obtainable under the Wiretap Act, the SCA, or the Pen/Trap Statute? The answer to this question is clearly ‘no.’”

In *In re Applications of U.S. for Orders Authorizing Disclosure of Cell Cite Info.*, 05-403, 2005 WL 3658531 (D.D.C. Oct. 26, 2005) (hereinafter *Robinson Op.*) that court held that “[f]or these reasons, the undersigned United States Magistrate Judge determined that the disclosure of cell site information is not authorized by [18 U.S.C.] Section 2703, by Sections 3122 and 3123, or by any combination of the two provisions.”

In *In re Application of U.S. for an Order Authorizing Installation & Use of a Pen Register & a Caller Identification Sys. on Tel. Numbers (Sealed)*, 402 F. Supp. 2d 597, 598 (D.

USA V. LOPEZ LOPEZ, ET AL.
 3:13-CR-00022-CVG-RM-4
 MOTION TO SUPPRESS — CELL SITE INFORMATION

Md. 2005) (hereinafter *Bredar Op.*) that court noted: “[t]he government also requested an order directing the relevant wireless communications service provider to disclose “real time cell site information,” which would reveal the physical location of the person in possession of the cell phone whenever the phone was on. The government did not seek information regarding the contents of any communication. After reviewing the government’s application, including proffered “specific and articulable facts showing ... reasonable grounds to believe that ... the records or other information sought [would be] relevant and material to an ongoing criminal investigation,” 18 U.S.C. 2703(d), and after reviewing the statutes referenced in the application, the court concluded the cited authority and the proffer were insufficient to support the government's request. The court determined the government needed to show probable cause in a sworn affidavit in order to obtain real time cell site information.).

In *In re Application of U.S. for an Order Authorizing the Release of Prospective Cell Site Info.*, 407 F.Supp. 2d 132, 133 (D.D.C. 2005) (hereinafter *Facciola Op. I*) Judge Facciola opined: “[m]ore to the point, the probable cause showing does not meet the central problem identified in the Texas⁵ and New York⁶ cases, that the statutes upon which the government purports to rely in those cases and in this one, *i.e.*, 18 U.S.C. §§ 3122, 3123, 2703(c)(1) do not authorize the government to secure cell site data that would disclose the location of the person using the cell phone. Invocation of the probable cause standard does not solve the fundamental problem that the statutes the government invokes cannot be construed to give the government the information it seeks.”

In *In re U.S. for an Order Authorizing the Release of Prospective Cell Site Info.*, 407 F. Supp. 2d 134, 135 (D.D.C. 2006) (hereinafter *Facciola Op. II*) Judge Facciola again addressed

⁵ See *Smith Op.*, *supra*.

⁶ See *Orenstein Op.*, *supra*.

USA V. LOPEZ LOPEZ, ET AL.
3:13-CR-00022-CVG-RM-4
MOTION TO SUPPRESS — CELL SITE INFORMATION

CSLI and stated: “[i]f one accepts, as I do, that, as three magistrate judges have held, (internal citation omitted) the information the government seeks can only be secured by a warrant issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure, the standard that pertains to the issuance is, as the Fourth Amendment requires, probable cause to believe that the information sought is itself evidence of a crime, not that the information is relevant to an investigation.”

In *In re U.S.*, 1:06-MC-6, 2006 WL 1876847 (N.D. Ind. July 5, 2006) (hereinafter *Lee Op.*) that court stated: “[t]his Court has reviewed the extensive writing that has already been committed to resolving this issue in other jurisdictions and has also given the matter independent consideration. The conclusion reached is the same as that of the Magistrate Judge in his Order denying the applications, specifically: (1) the Government cannot rely on the Pen Register Statute to obtain cell site location information; and (2) converging the Pen Register Statute with the SCA in an attempt to circumvent the exception in the CALEA is contrary to Congress’ intent to protect cell site location information from utilization as a tracking tool absent probable cause under the Fourth Amendment.”

In *In re U.S. For an Order Authorizing the Disclosure of Prospective Cell Site Info.*, 412 F. Supp. 2d 947, 958 (E.D. Wis. 2006) *aff’d*, 06-MISC-004, 2006 WL 2871743 (E.D. Wis. Oct. 6, 2006) (hereinafter *Callahan Op.*) Magistrate Callahan opined that: “[t]he bottom line is that the array of statutes invoked by the issues in this case, *i.e.*, the Pen/Trap Statute, the SCA, and CALEA present much more a legislative collage than a legislative mosaic. If Congress intended to allow prospective cell site information to be obtained by means of the combined authority of the SCA and the Pen/Trap Statute, such intent is not at all apparent from the statutes themselves. Indeed, for the reasons set forth above, the legislative history of CALEA would suggest

USA V. LOPEZ LOPEZ, ET AL.
3:13-CR-00022-CVG-RM-4
MOTION TO SUPPRESS — CELL SITE INFORMATION

Congress's intent to be otherwise. Accordingly, and for all of the foregoing reasons, the government's application will be denied."

And in *In Re U.S. for an Order: (1) Authorizing Installation & Use of Pen Register & Trap & Trace Device; (2) Authorizing Release of Subscriber & Other Info.; (3) Authorizing Disclosure of Location-Based Servs.*, CIV.A. MISC. -07-128, 2007 WL 3342243 (S.D. Tex. Nov. 7, 2007) (hereinafter *Owsley Op.*) that court said: "[t]he information that the Government seeks clearly attempts to identify the exact location of the Target Device (and presumably the person holding the Target Device), and thus requires a finding of probable cause."

Indeed, one case stands out for this Court's consideration – The District of Puerto Rico's decision in *In re Application of U.S. for Order*, 497 F. Supp. 2d 301 (D.P.R. 2007) (hereinafter *McGiverin Op.*). In the *McGiverin Op.*, like here, the Government filed applications under 18 U.S.C. §§ 2703 and 3122 and, like here, "the government's requests for cell site information are prospective in nature that is, the application seeks capture and disclosure of "geographic location information ... for a period not to exceed sixty (60) days from the date of this Court's order." *Id.* at 303. As Magistrate Judge McGiverin aptly noted:

There is another reason the SCA cannot be used as authority for disclosure of [CSLI]: the SCA's trail of definitions leads, inescapably in my judgment, to the conclusion that the discloseable information under the statute does not include location information. As indicated above, the provisions of the SCA apply to providers of an "electronic communications service," and the "information" that may be obtained must pertain to the customer of such "service." "Electronic communications service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Thus, in order for Section 2703(c) to apply, the information requested must pertain to "wire or electronic communications."

Those terms, however, cannot be read to encompass cell phone location data. First, "wire communication" is defined as "any aural transfer" which in turn is defined as "a transfer containing the

USA V. LOPEZ LOPEZ, ET AL.
3:13-CR-00022-CVG-RM-4
MOTION TO SUPPRESS — CELL SITE INFORMATION

human voice at any point between and including the point of origin and point of reception.” 18 U.S.C. §§ 2510(1), (18). Cell site data is not a wire communication under this definition because it does not involve the transfer of the human voice at any point along the path between the cell phone and the cell tower.

Nor can cell site data be considered an “electronic communication.” EPCA defines that term as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include ... any communication from a tracking device (as defined in section 3117 of this title).” 18 U.S.C. § 2510(12). The term “tracking device” is defined in EPCA as “an electronic or mechanical device which permits the tracking of the movement of a person or object.” 18 U.S.C. § 3117(b).

Id. at 310 (D.P.R. 2007) (some citations omitted and emphasis removed).

Ultimately Magistrate McGiverin *rejected* the Government’s attempt to obtain evidence via statutory authority (in contrast to a warrant issued pursuant to Rule 41). *See Id.* at 311 (“[f]inding the statutes proffered by the government insufficient to authorize the court to issue an order authorizing disclosure of prospective cell site information, the court ... is left with only the general authority to issue a Rule 41 warrant upon a showing of probable cause to believe that the data sought will yield evidence of a crime.”).

The Third Circuit has addressed Government applications for information under 18 U.S.C. § 2703. *In re Application of U.S. for an Order Directing a Provider of Elec. Comm’n Serv. to Disclose Records to Gov’t*, 620 F.3d 304, 305 (3d Cir. 2010) (*Slovitier Op.*). In that case, the Third Circuit noted that the Government sought historical cellular telephone data. *Id.* Here, in contrast, the Government sought prospective information. Moreover, the Third Circuit in the *Slovitier Op.* noted that:

The [Cell-Site Location Information] requested by the Government consists of records of information collected by cell towers when a subscriber makes a cellular phone call. That historical record is

derived from a “wire communication” and does not itself comprise a separate “electronic communication.” Thus, even if the record of a cell phone call does indicate generally where a cell phone was used when a call was made, so that the resulting CSLI was information from a tracking device, that is irrelevant here because the CSLI derives from a “wire communication” and not an “electronic communication.”

Id. at 310 (emphasis added).

So while instructive to this Court’s decision, the Circuit’s actual holding in the *Slovitier Op.* was: “[i]n sum, we hold that CSLI from cell phone calls is obtainable under a § 2703(d) order and that such an order does not require the traditional probable cause determination.” *Id.* at 313 (emphasis added). But here the Government sought information not when a cellular phone was only making a call; instead it was seeking information on a continuous and prospective basis in order to interdict a boat on the open water. *See Affidavit* at p. 5. This distinction is critically important here because absent a cellular telephone call there is no “wire communication” as defined by statute, instead it would be “electronic communications”, and since “tracking devices” are excluded from the definition of “electronic communications” the Government’s failure to get a warrant requires all evidence to be suppressed as fruit of the poisonous tree.

B. 4th Amendment Violation of Reasonable Expectation of Privacy

Recently, the Supreme Court in *United States v. Jones*, 132 S. Ct. 945 (2012) addressed the significance of property rights in Fourth Amendment search and seizure analysis, and detailed that “for most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas (‘persons, houses, papers, and effects’) it enumerates.” *Id.* at 950 (footnote omitted). However *Jones* in no uncertain terms stated that: “we do not make trespass the exclusive test. Situations involving merely the transmission of

USA v. LOPEZ LOPEZ, ET AL.
3:13-CR-00022-CVG-RM-4
MOTION TO SUPPRESS — CELL SITE INFORMATION

electronic signals without trespass would remain subject to *Katz*⁷ analysis.” *Jones*, 132 S. Ct. at 953.

Justice Sotomayor also remarked that: “[w]ith increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones.” *Id.* at 955 (Sotomayor, J. concurring). Justice Sotomayor ultimately “agree[d] with Justice Alito that, at the very least, ‘longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy,’ and that “[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to *Katz*⁷ analysis.” *Id.* (internal citations omitted).

Indeed, cell-site location information “is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: ‘limited police resources and community hostility.’” *Id.* at 956 quoting *Illinois v. Lidster*, 540 U.S. 419, 426 (2004).

Justice Sotomayor goes on to state: “I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.” *Id.* at 957. Under the concurring opinions in *Jones*, the evidence introduced at trial that derived from CSLI information should be suppressed under the Fourth Amendment for failure to obtain a search warrant, as the evidence violated the cellular telephone holder’s reasonable expectation of privacy.

The Sixth Circuit has taken this commonsense approach in the context of emails in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). In *Warshak*, the court held “that a subscriber enjoys a reasonable expectation of privacy in the contents of emails ‘that are stored

⁷ *Katz v. United States*, 389 U.S. 347 (1967).

USA v. LOPEZ LOPEZ, ET AL.
 3:13-CR-00022-CVG-RM-4
 MOTION TO SUPPRESS — CELL SITE INFORMATION

with, or sent or received through, a commercial [Internet Service Provider] ISP.’ The government may not compel a commercial ISP to turn over the contents of a subscriber’s emails without first obtaining a warrant based on probable cause. Therefore, because they did not obtain a warrant, the government agents violated the Fourth Amendment when they obtained the contents of Warshak’s emails. Moreover, to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional.” *Id.* at 288. There is not logical distinction between emails sent via ISPs and CSLI information sent to CSP. Accordingly, the failure to obtain a warrant in this case is fatal and the evidence obtain therefrom must be suppressed.

The Supreme Court has over a decade ago recognized that advances in “police technology [can] erode the privacy guaranteed by the Fourth Amendment.” *Kyllo v. United States*, 533 U.S. 27, 34 (2001). Indeed, Judge Kozinski in dissenting from the denial of a petition for rehearing *en banc* in *United States v. Pineda-Moreno*, 617 F.3d 1120 (9th Cir. 2010) observed: “[t]he Supreme Court in *Knotts*⁸ expressly left open whether “twenty-four hour surveillance of any citizen of this country” by means of “dragnet-type law enforcement practices” violates the Fourth Amendment’s guarantee of personal privacy. When requests for cell phone location information have become so numerous that the telephone company must develop a self-service website so that law enforcement agents can retrieve user data from the comfort of their desks, we can safely say that “such dragnet-type law enforcement practices” are already in use.” *Id.* at 1126 (internal citation omitted). Here the Government applied for and obtained the Order allowing the target cell phones to be tracked for 60 days. This is exactly the type of dragnet law enforcement practice that the Supreme Court rejected in *Knotts*, and was

⁸ *U.S. v. Knotts*, 460 U.S. 276 (1983).

USA v. LOPEZ LOPEZ, ET AL.
3:13-CR-00022-CVG-RM-4
MOTION TO SUPPRESS – CELL SITE INFORMATION

rejected, yet again, by Justice Alito in *Jones*. See *Jones*, 132 S. Ct. at 964 (Alito, J. concurring) (“[w]e need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4–week mark.”).

The calendar is clear - 60 days is long past the 28 days rejected by Justice Alito. See also *In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d 113, 127 (E.D.N.Y. 2011) “[w]hile the government’s monitoring of our thoughts may be the archetypical Orwellian intrusion, the government’s surveillance of our movements over a considerable time period through new technologies, such as the collection of cell-site-location records, without the protections of the Fourth Amendment, puts our country far closer to Oceania than our Constitution permits.”).

Indeed, just last month the New Jersey Supreme Court held on independent state grounds that “cell-phone users have a reasonable expectation of privacy in their cell-phone location information, and that police must obtain a search warrant before accessing that information.” *State v. Earls*, --- A.3d ---, 2013 WL 3744221 (N.J. July 18, 2013).

CONCLUSION

Consequently, the Government’s acquisition of CSLI was a technological panopticon that was obtained in contravention of the PSR, the SCA, and the CALEA and also violated the Defendant’s 4th Amendment rights. All evidence obtained from the Order, and all fruits thereof, must be suppressed.

WHEREFORE the Defendant respectfully requests that the Court enter an Order suppressing all evidence the Government obtained from the April 13, 2013, Order and all evidence derived therefrom.

USA v. LOPEZ LOPEZ, ET AL.
3:13-CR-00022-CVG-RM-4
MOTION TO SUPPRESS — CELL SITE INFORMATION

Dated: *August 8, 2013*

CEVALLOS & WONG, LLP


/s/ Daniel Cevallos

Daniel Cevallos, Esquire
Virgin Islands Bar ID No.: 1154
Tel: (267) 639-3105
Fax: (215) 689-4375
danny@cevalloswong.com

USA V. LOPEZ LOPEZ, ET AL.
3:13-CR-00022-CVG-RM-4
MOTION TO SUPPRESS — CELL SITE INFORMATION

Certificate of Service

I hereby certify that on the day below, a true copy of the foregoing **MOTION TO SUPPRESS CELL SITE INFORMATION** was electronically filed with the Clerk of the Court using the CM/ECF System, which will send a notification of such filing (NEF) to the following:

Kelly B. Lake
Kim Lindquist
United State Attorney's Office
Federal Building & U.S. Courthouse
5500 Veterans Drive
Suite 260
St Thomas, VI 00802
Email: Kelly.Lake2@usdoj.gov

Gabriel J. Villegas
Edson A Bostic
Federal Public Defender
1019 Beltjen Place Suite 1
P.O. Box 1327
St. Thomas, VI 00822-3450
Email: gabriel_villegas@fd.org

Robert L. King
Birch, Dejongh & Hindels
1330 Estate Taarnberg
St. Thomas, VI 00802
Email: rlking@attyking.com

Treston E Moore
Moore, Dodson & Russell, P.C.
P.O. Box 310, E.G.S. (14A Norre Gade)
St. Thomas, VI 00804-0310
E-mail: tresmoore@aol.com

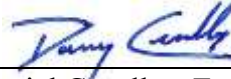
Arturo R. Watlington, Jr.
Law Offices of Arturo Watlington
#3 Store Gronne Gade
P.O. Box 261
St. Thomas, VI 00804
arwatlington@yahoo.com

Nizar A. DeWood
The Dewood Law Firm
2006 Eastern Suburb, Suite 101
Christiansted, VI 00820
dewoodlaw@me.com

Joseph DiRuzzo, Esquire
Fuerst Ittleman David Joseph
1001 Brickell Bay Drive
32nd Floor
Miami, Florida 33131
jdiruzzo@fuerstlaw.com

Dated: *August 8, 2013*

CEVALLOS & WONG, LLP



Daniel Cevallos, Esquire
Virgin Islands Bar ID No.: 1154
1420 Walnut Street, Suite 1012
Philadelphia, PA 19102